UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

SHARYL THOMPSON ATTKISSON, JAMES HOWARD ATTKISSON, SARAH JUDITH STARR ATTKISSON, Plaintiffs, v. ERIC HOLDER, Individually, PATRICK R. DONAHOE, Individually, UNKNOWN NAMED AGENTS OF THE DEPARTMENT OF JUSTICE, in their individual capacities, UNKNOWN NAMED AGENTS OF THE UNITED STATES POSTAL SERVICE, in their individual capacities, UNKNOWN NAMED AGENTS OF THE UNITED STATES, in their individual Capacities, Defendants.	Civil Action No. 1:17-cv-364-LMB

PLAINTIFFS' CONSOLIDATED COMPLAINT

Plaintiffs, by and through undersigned counsel, submit the following Consolidated Complaint pursuant to the Court's September 14, 2017 Order [Docket No. 114).

1. Counts 1 and 2 are brought pursuant to *Bivens*[1] and challenge the government's unauthorized and illegal surveillance of the Plaintiffs' laptop computers and telephones from 2011-2014 under the First Amendment to the United States Constitution and the Fourth Amendment to the United States Constitution. The allegations are made against Defendants in their individual capacity and not their official capacity.

2. Counts 3 through 8 are brought through and pursuant to the Federal Tort Claims Act ("FTCA"), 28 U.S.C. § 2671 *et seq*., the United States Constitution, and the law of the Commonwealth of Virginia.

JURISDICTION

3. The subject litigation arises under the Constitution and laws of the United States, and the Court has jurisdiction over the subject matter of this Complaint under 28 U.S.C. §§ 1331 & 1346(b).

4. On December 26, 2014, Plaintiffs submitted an Administrative Tort Claim to the United States Department of Justice and the United States Postal Service as required by law. Plaintiffs' claim was deemed denied by virtue of Claimants/Plaintiffs receiving no response from the respective federal agencies within six months of filing, pursuant to 28 U.S.C. § 2675(a). Plaintiffs have therefore exhausted all available administrative remedies, and satisfied all conditions precedent, to the filing of suit.

PARTIES

5. Plaintiffs incorporate and re-allege each and every allegation above as if fully set

[1] *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics,* 403 U.S. 388 (1971). *Bivens* action is now regarded as the federal equivalent to 42 U.S.C. § 1983, which permits state officials to be sued for violations of individuals' constitutional rights.

forth herein, including the allegations in the original complaint.

6. At all times relevant to the subject lawsuit, separate Plaintiff Sharyl Attkisson is, and was, a citizen and resident of Leesburg, Virginia, and an investigative reporter for CBS News. Plaintiff was responsible for investigating, writing, publishing, and airing investigative news stories on a wide-variety of topics, including the federal gun-trafficking investigation that came to be known as *"Fast and Furious,"* and the controversial attack of the American diplomatic mission in Benghazi, Libya. At all times relevant hereto, Ms. Attkisson was a member of "the press" as described by the First Amendment to the Constitution of the United States. In the course of her investigative journalism, she experienced confrontational encounters with officials within the DOJ and White House who demanded disclosure of the identity of confidential sources who may have been leaking information. Federal agencies and the White House repeatedly withheld documents, at times invoking "national security" as justification. During the same time period, the DOJ implemented efforts to vastly expand its cyber security capabilities, efforts, and resources in the name of national security, including actively targeting journalists and news organizations as part of leak investigations. Ms. Attkisson discovered that her computers and telephone had been hacked or compromised remotely, and that an unauthorized party or parties had illegally infiltrated her electronics and placed software on her laptop computer, and that her confidential, professional, and personal information had been illegally accessed, compromised, and infiltrated.

7. At all times relevant to the subject lawsuit, Plaintiff James Howard Attkisson is and was a citizen and resident of Leesburg, Virginia, and was married to Sharyl Attkisson. Because much of the surveillance alleged in this complaint occurred at Ms. Attkisson's

residence, Mr. Attkisson was subjected to surveillance as well, and his confidential, professional, and personal information was illegally accessed.

8. At all times relevant to the subject lawsuit, Plaintiff Sarah Judith Starr Attkisson was a citizen and resident of Leesburg, Virginia, and the daughter of James and Sharyl Attkisson. Because much of the surveillance alleged in this complaint occurred at Sarah Attkisson's residence, she was subjected to surveillance as well, and her confidential, professional, and personal information were illegally accessed.

9. At all times relevant to the subject litigation, Defendant Eric H. Holder was the Attorney General of the United States. Defendant Holder served as the 82nd Attorney General between 2009 and 2015. He was appointed by President Obama. Between 2009 and 2015, Defendant Holder had ultimately authority over, among others, the Department of Justice ("DOJ") and the FederalBureau of Investigation ("FBI"). He is sued herein in his individual capacity only for his own conduct. The position of Attorney General was created by the Judiciary Act of 1789. In June, 1870, Congress enacted a law entitled "*An Act to Establish the Department of Justice*." The Act established the Attorney General as head of the Department of Justice (DOJ) and gave the Attorney General direction and control of U.S. Attorneys and all other counsel employed on behalf of the United States. The Act also vested in the Attorney General supervisory power over the accounts of U.S. Attorneys and U.S. Marshals. The mission of the Office of the Attorney General is to supervise and direct the administration and operation of the DOJ, including the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Bureau of Prisons, Office of Justice Programs, and the U.S. Attorneys and U.S. Marshals Service, which are all within the Department of Justice.

The principal duties of the Attorney General include representing the United States in legal matters; supervising and directing the administration and operation of the offices, boards, divisions, and bureaus that comprise the Department; furnishing advice and opinions, formal and informal, on legal matters to the President and the Cabinet and to the heads of the executive departments and agencies of the government, as provided by law; making recommendations to the President concerning appointments to federal judicial positions and to positions within the Department, including U.S. Attorneys and U.S. Marshals; representing or supervising the representation of the United States Government in the Supreme Court of the United States and all other courts, foreign and domestic, in which the United States is a party or has an interest as may be deemed appropriate; and performing or supervising the performance of other duties required by statute or Executive Order.

10. Between 2011 and 2015, Defendant Patrick R. Donahoe served as the 73rd Postmaster General and Chief Executive Officer of the United States Postal Service ("USPS") with ultimate authority over the USPS. He is sued herein in his individual capacity only for his own conduct. The USPS was established as an independent establishment within the executive branch of the Government under the provisions of the Postal Reorganization Act of August 12, 1970, Pub. L. 91-375. The Board of Governors of the Postal Service directs the exercise of powers of the USPS, reviews the practices and policies of the Postal Service, and directs and controls its expenditures. The Postmaster General (PMG) is the chief executive officer of the USPS and is responsible by law for its overall operations. The PMG is named and can be removed by a majority of the nine Governors. Pursuant to law, the PMG is authorized to direct any officer, employee, or agent of the Postal Service to exercise such of the PMG's powers as the PMG deems appropriate.

11. Plaintiffs are unaware of the true names and capacities, whether individual or otherwise, of the Unknown Federal Agents referenced in the caption and therefore sue the unnamed Defendants by fictitious names. Plaintiffs are informed and believe, and on that basis, allege, that these Defendants, and each of them, are in some manner responsible and liable for the acts and/or damages alleged inthe Complaint, and that these Defendants, including all Defendants, are and were employees or agents of the federal government who acted under color of law, and that each subjected Plaintiffs to, or caused them to be subjected to, constitutional violations and damages from Defendants' tortious actions.

BACKGROUND

12. The First Amendment protects the rights of American citizens to engage in free and open discussions, and to associate with persons of their choosing, and the Fourth Amendment guarantees that citizens will be free of unreasonable searches and seizures. Defendants herein have expressly interfered with those rights. More importantly, Defendants alleged activities in the aggregate have served to deter the exercise of First Amendment rights by those who become aware of the covert operations.

13. The facts alleged herein, and those referenced from public sources, demonstrate a clear and present danger to our most fundamental protections as a result of an intelligence community employing surreptitious collection techniques, including highly sophisticated forms of electronic surveillance, to achieve overly broad intelligence targeting and collection objectives in violation of law.

14. During all times relevant to the subject Complaint, Ms. Attkisson was an investigative reporter for CBS News. She served CBS for twenty (20) years. Her job required her to investigate

and report on national news stories. In 2011, during the course of her reporting, Plaintiff began investigating what later became known as the *"Fast and Furious"* gun-walking story[2] involving federal agents from the Bureau of Alcohol, Tobacco, and Firearms (ATF) improperly permitting weapons to pass into the hands of the Mexican drug cartels.

15. Her first *Fast and Furious* report aired on CBS on February 22, 2011. The report quoted and relied upon numerous confidential sources, all of whom were critical of the*Fast and Furious* gun-walking strategy deployed by the respective federal agencies.

---

[2] The "Gunwalking", or "letting guns walk", was a tactic of the United States Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), which ran a series of sting operations between 2006 and 2011 in the Tucson and Phoenix area where the ATF purposely allowed licensed firearms dealers to sell weapons to illegal straw buyers, hoping to track the guns to Mexican drug cartel leaders and arrest them. The operations were done under the umbrella of *Project Gunrunner*, a project intended to stem the flow of firearms into Mexico by interdicting straw purchasers and gun traffickers within the United States. The Jacob Chambers Case began in October 2009 and eventually became known in February 2010 as "Operation Fast and Furious" after agents discovered Chambers and the other suspects under investigation belonged to a car club. The desired goal of allowing these purchases was to continue to track the firearms as they were transferred to higher-level traffickers and key figures in Mexican cartels, with the expectation that this might lead to arrests and dismantling of the cartels. The tactic was questioned during the operations by a number of people, including ATF field agents and cooperating licensed gun dealers. During Operation *Fast and Furious*, the largest "gunwalking" probe, the ATF monitored the sale of about 2,000 firearms, of which only 710 were recovered as of February, 2012. A number of straw purchasers were arrested and indicted; however, as of October, 2011, none of the targeted high-level cartel figures had been arrested. Guns tracked by the ATF were found at crime scenes on both sides of the Mexico–United States border, and the scene where United States Border Patrol Agent Brian Terry was killed in December, 2010. The "gunwalking" operations became public in the aftermath of Terry's murder. Dissenting (whistleblowing) ATF agents came forward to Congress in response. According to Humberto Benítez Treviño, former Mexican Attorney General and chair of the justice committee in the Chamber of Deputies, related firearms were found at numerous crime scenes in Mexico where at least 150 Mexican civilians were maimed or killed. Revelations of "gunwalking" led to controversy in both countries, and diplomatic relations were damaged. As a result of a dispute over the release of Justice Department documents related to the scandal, Attorney General Eric Holder became the first sitting member of the Cabinet of the United States to be held in contempt of Congress on June 28, 2012. Earlier that month, President Barack Obama had invoked executive privilege for the first time in his presidency over the same documents.

16. In February, 2011, the ATF, in an internal memorandum, instigated an orchestrated campaign against Ms. Attkisson's report, including efforts to discredit it, and outlined a strategy for the Agency to push "positive stories" in order to "preempt some negative reporting."[3]

17. Despite the foregoing efforts, Ms. Attkisson continued to report *Fast and Furious* stories. When contacted for comment, DOJ officials persisted in their denial of the allegations and continued efforts to unveil Ms. Attkisson's confidential sources. ATF sources told Ms. Attkisson that the Agency was actively seeking to identify government insiders who were providing information or "leaking" to her and CBS.

18. In September, 2011, Ms. Attkisson reported on secret audio recordings that implicated the FBI in an alleged discrepancy in its accounting of evidence in the *Fast andFurious* related murder of Border Patrol Agent Brian Terry.

19. The referenced reporting by Plaintiff Attkisson was public reporting available both on television and online.

20. Also in September, 2011, Ms. Attkisson reported on the alleged involvement of an F.B.I. informant in the *Fast and Furious* matter.

21. In October, 2011, Ms. Attkisson reported on the continuing controversy regarding the F.B.I.'s accounting of evidence in *Fast and Furious.*

---

[3] See http://www.cbsnews.com/8301-31727_162-20039251-10391695.html
"Given the negative coverage by CBS Evening News last week and upcoming events this week, the bureau should look for every opportunity to push coverage of good stories. Fortunately, the CBS story has not sparked any follow up coverage by mainstream media and seems to have fizzled….It was shoddy reporting… ATF needs to proactively push positive stories this week, in an effort to preempt some negative reporting, or at minimum, lessen the coverage of such stories in the news cycle by replacing them with good stories about ATF."

22. In November, 2011, Ms. Attkisson reported on evidence contradicting Attorney General Holder's sworn testimony wherein he claimed that he had only heard of *Fast and Furious* for the first time in the past couple of weeks.

23. In mid-to-late 2011, Ms. Attkisson, Mr. Attkisson, and Sarah Attkisson began to notice anomalies in numerous electronic devices at their home in Virginia. These anomalies included a work Toshiba laptop computer and a family Apple desktop computer turning on and off at night without input from anyone in the household, the house alarm chirping daily at different times, often indicating "phone line trouble," and television problems, including interference. All of the referenced devices use the Verizon FiOS line installed in Ms. Attkisson's home. Verizon was unable to cure the problems, despite multiple attempts over a period of more than a year.

24. In December, 2011, Ms. Attkisson reported on the DOJ's formal retraction of a letter and a misrepresentation made to Congress in February, 2011, which had stated, incorrectly, there had been no "gun-walking."

25. In January, 2012, Ms. Attkisson contacted Verizon about ongoing internet problems and intermittent connectivity because the residential internet service began constantly dropping off. She had not experienced similar problems previously. In response to the complaint, Verizon sent a new router, which was immediately installed. The new router failed to resolve the issues.

26. In January, 2012, Ms. Attkisson began a series of reports, spanning several months, which were critical of the Executive Branch's green energy initiatives, including the Solyndra failure.

27. In February, 2012, an unauthorized party or parties remotely installed sophisticated surveillance spyware on Ms. Attkisson's Toshiba laptop. The invasion was obviously unknown to

Ms. Attkisson at the time, but revealed later by forensic computer analysis, including factual evidence demonstrating that Plaintiffs' computer systems were targets of unauthorized surveillance efforts, including prolonged ongoing surveillance of the iMac. From artifacts remaining on the iMac, the intrusions were occurring as early as June, 2011. The forensic analysis likewise revealed direct targeting of Plaintiffs' Blackberry mobile phone when connected to the iMac. Records reveal a file recovery process performed by an intruder that transferred large numbers of records off the BlackBerry. Changes to VPN settings were likewise found as the enabling of the built in Ethernet connection, after years of not being used, reflect further clear evidence of unauthorized surveillance activities. The issuing of the *smbclient* command along with recovered records showing the iMac mounted as a network shared resource, is further evidence of uninvited, remote surveillance designed to enable the contents on the iMac to be easily exposed as well as exfiltrated. From the available forensic evidence, the unauthorized intruder maintained complete control of the system. Access to e-mails, personal files, Internet browsing, passwords, execution of programs, financial records, photographs of not just the Client but of the Client's family members was likewise achieved. With regard to attribution, information recovered directly from Plaintiffs' computer proved that remote communication with Client's system was executed via an IP address owned, controlled, and operated by the United States Postal service, and was not associated with any web server or website used by the USPS. Attempts to communicate with the IP address were rejected. The IP address was not a random find on the computer, nor was it found in the Internet browsing history. Analysis demonstrated that there was a communications channel opened up between the referenced IP address and Client's computer thus establishing undisputable evidence that a person using the IP address, which is part of the federal government, was communicating directly with Client's computer on an

ongoing basis during the times in question.

28. In February, 2012, Ms. Attkisson contacted Verizon yet again to complain about continuing anomalies.

29. In March, 2012, a Verizon representative visited Ms. Attkisson's home and replaced the router a second time. The representative also replaced the entire outside FiOS service box. Despite Verizon's efforts, however, the anomalies persisted.

30. In April-May, 2012, the DOJ and FBI publicly announced a new effort to vastly expand cyber related efforts to address alleged "national security-related cyber issues." During the same time frame, the DOJ secretly--and without notice--seized personal and phone records belonging to journalists from the Associated Press news agency in violation longstanding DOJ practice. The records seizure was not publicly known at the time, but was later revealed.[4]

31. In July, 2012, the DOJ designated U.S. Attorneys' offices to act as "force multipliers" in its stepped-up cyber efforts in the name of national security.[5]

32. That same month, July, 2012, intruders remotely "refreshed" the ongoing surveillance of Ms. Attkisson's Toshiba computer. Again, the access was unknown to Ms.Attkisson at the time, but was revealed later through computer forensic analysis.

33. In September, 2012, Wikileaks published internal emails from a global intelligence company doing business with government agencies. The materials made reference to"Obama leak investigations" and the alleged "witch hunts of investigative journalists learning information from inside the beltway sources." The email states, "(T)here is a specific tasker fromthe [White House]

---

4 http://blogs.justice.gov/main/archives/date/2012/11

5 http://www.wikileaks.org/gifiles/docs/1210665_obama-leak-investigations-internal-use-only-pls-do-not.html (last accessed on October 28, 2014).

to go after anyone printing materials negative to the Obama agenda (oh my.) Even the FBI is shocked."

34. On October 5, 2012, CBS aired Ms. Attkisson's first Benghazi story for CBS, which was critical of the Executive Branch's handling of the security requests at the U.S. compound in Benghazi, Libya, where Ambassador Christopher Stevens and three (3) other U.S. personnel were killed on September 11, 2012.

35. On October 8, 2012, CBS aired another Attkisson report on Benghazi that included an interview with whistleblower Col. Andrew Wood. During the weeks following the airing of Col. Wood's interview, Ms. Attkisson made personal contact with numerous confidential sources within the federal government (or who had links to intelligence agencies within the U.S. government). The confidential government sources reported to Ms. Attkisson that efforts were being made by the Executive Branch to clamp down on leaks and to track the leaking of information to specific reporters regarding the Benghazi affair.

36. During the same time period, October of 2012, the DOJ continued its stepped-up cyber efforts with its National Security Division providing specialized training at DOJ headquarters for the National Security Cyber Specialists (NSCS) network and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS).

37. In the later part of October 2012, Ms. Attkisson, Mr. Attkisson, and Sarah Attkisson began noticing an escalation of electronic problems at their personal residence, including interference in home and mobile phone lines, computer interference, and televisioninterference. They were still unaware of any intrusion, however.

38. During the same general time frame, several sources with close ties to the

intelligence community approached Ms. Attkisson privately and informed her that the government would likely be monitoring her electronically in an effort to identify her confidential sources, and also to monitor her continued *Fast and Furious* and *Benghazi* stories.

39. From November 7-9, 2012, Attorney General Holder hosted a national training conference at DOJ headquarters for the expanded efforts of DOJ's National Security Cyber Specialists (NSCS).[6] On November 13, 2012, the F.B.I. initiated a body of cyber security case investigations that would later relate to the illegal intrusions directed at Ms. Attkisson.

40. In November 2012, Ms. Attkisson's phone line became nearly unusable because of anomalies and interruptions. Her mobile phones also experienced regular interruptions and interference, making telephone communications unreliable, and, at times, virtually impossible.

41. In December 2012, Ms. Attkisson discussed her phone and computer issues with

---

[6] "With the network built, the [Justice] department will be able to accelerate some of the national security cyber work that has been ongoing since [National Security Division's] cyber review." "To equip this large cyber cadre in how to best address these new threats, the department has developed and carried out extensive training. Last week's inaugural NSCS conference covered topics ranging from digital evidence, to the Foreign Intelligence Surveillance Act, to current threat trends, to common challenges in combating national security cyber threats specifically. Underscoring the importance of this mission, Attorney General Eric Holder, FBI Director Robert Mueller, Assistant Attorney General Monaco, and others from the department and the FBI addressed the network throughout the three-day conference. .. the network will help strengthen partnerships between the department and agencies across the U.S. government, including the Department of Homeland Security, the Department of Defense, and various elements of the Intelligence Community. The network also will work particularly closely with the FBI's National Cyber Investigative Joint Task Force (NCIJTF) to help preserve all intelligence collection, prevention, disruption and response options for cyber national security threats. ..Going forward, the NSCS network is focused on ensuring a whole-of-government and all-tools approach to combating cyber threats to national security. The network will be working to bring investigations and prosecutions as viable options for deterrence and disruption as part of the government-wide response to these threats. The network will also be advising and consulting other parts of the government in the use of additional tools to counter these threats."
http://blogs.justice.gov/main/?s=NSCS%2C+specialized+training&search.x=25&search.y=16

friends, contacts, and sources, via her home phone, mobile phones, and email. She decided to begin logging the times and dates that the computers turned on at night without her input. Soon after these phone and email discussions, the computer nighttime activity stopped.

42. Computer forensic analysis later revealed that the intruders executed remote actions in December, 2012, to remove evidence of the intrusion from Ms. Attkisson's computers and home electronic equipment.

43. In December, 2012, a contact with U.S. government intelligence experience conducted an inspection of Ms. Attkisson's exterior home. During the course of the inspection, the consultant discovered an anomaly with Ms. Attkisson's FiOS (Verizon) box: an extra fiber optics line was dangling from the exterior of the box. Based on the odd finding, Ms. Attkisson contacted Verizon on December 31, 2012, which denied it had installed or had knowledge of the extraneous fiber optics line affixed to the equipment at the Attkisson's home and suggested Attkisson contact law enforcement authorities. Shortly thereafter, a person identifying herself as a Verizon supervisor telephoned Ms. Attkisson to advise her she was dispatching a technician to the house. It would be New Year's Day, so Ms. Attkisson informed the purported supervisor that it was unnecessary to dispatch a technician just then, and she offered to send them a photograph of the stray fiber optics line to save Verizon the trip. The purported supervisor declined the photograph and insisted that a technician would be present on New Year's Day.

44. On January 1, 2013, a person represented to be a Verizon technician visited the Attkisson's home and removed the additional fiber optics cable from the system. Ms. Attkisson asked the technician toleave the cable. The technician placed it next to the equipment and left the home. When Ms. Attkisson's husband arrived home and went to retrieve the extraneous cable, the

cable had already been removed and was no longer on the premises.

45. Throughout the month of January, 2012, Ms. Attkisson repeatedly contacted the purported Verizon technician to seek the location of the missing cable. The person representing himself as a technician never returned any of the calls at the number he had provided.

46. In January and February of 2013, Plaintiffs continued to experience phone and internet usage issues, including drop-offs, noises, and other interference. Verizon was notified and technicians and supervisors made additional contacts and visits.

47. On January 8, 2013, Ms. Attkisson made arrangements to deliver her Toshiba laptop to an individual with special expertise in computer forensics. On January 9, 2013, the forensics expert reported to Ms. Attkisson that the Toshiba laptop showed clear evidence of outside and unauthorized "intrusion," and that the sources of the intrusion were state-supported due to the sophisticated nature of the technology used.

48. On January 10, 2013, the computer was returned to Ms. Attkisson, along with a report. According to the report, the forensics computer expert found that sophisticated software had been used to accomplish the intrusion, and the software fingerprint indicated the software was proprietary to the federal government. The intrusion included, among other surveillance, keystroke monitoring, exfiltration of data, audio surveillance of Plaintiffs' conversations and activities at home by activating Skype, mining personal passwords, monitoring work and personal email, and probable compromise of Plaintiffs' work and personal smartphones. According to the report, the surveillance by the identified software spanned most of 2012 at least. The report also stated the intruders had accessed CBS network systems, such as the ENPS program, and that the perpetrator had also placed three (3) classified documents deep in the computer's operating system. Ms. Attkisson thereafter

notified her direct supervisor at CBS News of the laptop intrusion and findings.

49. On February 2, 2013, an independent forensic computer analyst retained by CBS News spent approximately six (6) hours at Ms. Attkisson's home, during which time he reported finding evidence on both Ms. Attkisson's Toshiba laptop and Apple desktop computers of a coordinated, highly-skilled series of actions and attacks directed at the operation of the computers and the storage and access of data thereon. CBS engaged the company to do further analysis of the Toshiba laptop in an attempt to recover wiped data.

50. In March 2013, Ms. Attkisson's Apple desktop computer began malfunctioning and, after several days of it freezing and emitting a burning odor, it shut down. Ms. Attkisson was unable to turn the Apple computer back on after this event.

51. On April 3, 2013, Ms. Attkisson filed a complaint with the DOJ Inspector General.

52. On May 6, 2013, an official with the United States Inspector General's office called Ms. Attkisson and stated that he had checked with the FBI, and the FBI denied any knowledge of any operations concerning Ms. Attkisson's computers or phone lines. The official also stated that there was no PATRIOT Act related order authorizing surveillance of Ms. Attkisson.

53. On May 21, 2013, Ms. Attkisson publicly stated in a radio interview her belief that her computers had been compromised, but did not assign or allege responsibility. A news outlet sought a statement from the DOJ regarding Ms. Attkisson's assertions. The DOJ issued a written response stating, "To our knowledge, the Justice Department has never compromised Ms. Attkisson's computers, or otherwise sought any information from or concerning any telephone, computer or other media device she may own or use."

54. On June 10, 2013, the independent cyber security firm hired by CBS confirmed that

there was a highly sophisticated intrusion into Ms. Attkisson's computer, as well as remote actions in December, 2012, to delete all evidence of the intrusion.

55. On June 11, 2013, CBS News issued a public statement, based on the forensics report, confirming that Ms. Attkisson's computer was accessed by an unauthorized, external, unknown party on multiple occasions in late 2012, and that the party used sophisticated methods to attempt to remove all possible indications of unauthorized activity.

56. The DOJ Inspector General requested a copy of the CBS forensic expert's report and requested the opportunity to examine the Toshiba computer. CBS denied the requests. Ms. Attkisson then retained an independent computer forensics expert to conduct further analysis of the Toshiba computer.

57. In September, 2013, while Ms. Attkisson continued working on the *Benghazi* story at her home in the evening, she observed for the first time that a third computer, her personal MacBook Air, was accessed remotely, controlled, and the data deleted.

58. In June of 2013, though Plaintiffs were unaware at the time, the FBI had begun conducting inquiries of Ms. Attkisson's computer intrusions under the auspices of a national security issue, but the agency failed to contact or interview Plaintiffs. Ms. Attkisson only discovered the FBI inquiry in December, 2013, when she appealed denial of her Freedom of Information Act request to the FBI and received some documents.[7]

59. The F.B.I. investigation involving Ms. Attkisson's computer intrusions was circulated to the DOJ's national cyber security group and included with a set of cases opened in November,

[7] Ms. Attkisson was unaware of the F.B.I. case at the time it was opened and for months thereafter.

2012, during the DOJ's expansion of its cyber team and the announcement of its intention to use "new tools" in its arsenal.

60. Although CBS did not release the compromised CBS computer to the DOJ Inspector General, in January, 2014, Ms. Attkisson agreed to release her personal Apple desktop computer to the DOJ Inspector General for analysis. During the investigation, the investigators remarked to the Plaintiff that they saw a great deal of suspicious activity on the computer. However, as months went by, the DOJ Inspector General refused to release a written report to Ms. Attkisson. The DOJ Inspector General also failed to properly respond to Ms. Attkisson's subsequent Freedom of Information Act requests on the topic. The DOJ Inspector General finally released a partial report upon Congressional request on the eve of Ms. Attkisson's testimony to a Senate panel in early 2015. Although the summary noted a great deal of advanced mode computer activity not attributable to Ms. Attkisson or anybody in her household, the report nonetheless concluded, paradoxically, that it found no evidence of intrusion in her personal Apple computer. The report was provided by government officials to the press. The report did not examine the compromised CBS laptop computer.

61. On January 16, 2014, and January 27, 2014, the head of the DOJ Inspector General Computer Forensics unit and a colleague visited Ms. Attkisson's home as part of the investigation, which included analysis of the Apple desktop.

62. Among other findings, Ms. Attkisson's computer forensics expert has identified an unauthorized communications channel opened into her Toshiba laptop directly connected to an Internet Provider (IP) address belonging to a federal government agency, specifically the United States Postal Service, indicating unauthorized surveillance whose source is the federal government.

63. The analysis shows the connection to a federal government agency was in use prior to January 8, 2013. The USPS has been publicly reported, including in IG internal audits, to have a working relationship with the FBI, Department of Homeland Security, and DOJ for domestic surveillance projects.

64. Ms. Attkisson's analyst also found that while the government source who first analyzed the Toshiba laptop in January, 2013, wiped evidence, there are indications that he or she likely copied and retained the evidence on an external hard drive.

65. Ms. Attkisson's analyst also found that direct evidence pointing to attribution for Ms. Attkisson's computer intrusions may also reside on the CBS network computer systems.

66. The above-cited events, which offer only brief highlights of the cyber-attacks suffered in Plaintiffs' home, caused Plaintiffs to incur unreasonable and unnecessary expenses in an effort to diagnose and correct the problems resulting from the attacks and intrusions; resulted in an invasion of their personal and family privacy; caused them to fear for their individual and family's well-being and safety; interfered with their ability to use their telephones, computer, and television; caused them fear for her sources' well-being and safety; interfered with Plaintiffs' ability to maintain necessary contacts with sources to perform her professional investigative reporting duties as a member of the press; affected Plaintiffs' sources' willingness to communicate with her; distracted from her duties as an investigative reporter; and resulted in irreparable tension in her relationship with her employer.

67. The actions of personnel working on behalf of the United States as described above, including the government intrusions, negligently, recklessly, and intentionally caused Plaintiffs' rights to privacy to be violated, and trespassed upon Plaintiffs' real and personal property as alleged

herein, without probable cause or any other legal justification, and as a result, Plaintiffs suffered damages.

68. The actions of the government employees and/or agents constitute violations of applicable law. Under the FTCA, the United States of America is liable for misconduct and actions of its agents and employees.

69. Defendants acted under color of law when conducting surveillance on the Plaintiffs and inhibiting the exercise of their First Amendment rights.

70. The surveillance of Plaintiffs' computers and telephones violated the Plaintiffs' right to privacy and trespassed upon their real and personal property. By subjecting Plaintiffs to surveillance of Ms. Attkisson's investigative efforts, Defendants sought to abridge the freedom of the pressand chill the exercise of the Plaintiffs' free speech in a reckless manner with objective unreasonableness, and with the intent to violate their rights.

71. The violation of Plaintiffs' right to privacy, and Constitutional rights, and the trespass upon Plaintiffs' real and person property proximately caused injuries, as set forth herein.

72. At all times relevant to the subject Complaint, the Defendants acted with reckless and callous indifference to the rights of Plaintiffs with the intent to subject them to, or cause them to be subjected to, constitutional violations. The actions included, among other things, the following acts:

A. Under the direction and policies created by the personal conduct of Defendant Holder, the Justice Department, and agencies for which he controlled, took unprecedented steps to chill and violate constitutional freedom of the press, including direct violations of Plaintiffs' constitutional rights and liberties. Defendant Holder's personal agenda and action as Attorney General included a targeted attack on whistleblowers and members of the press who have the personal and professional responsibility to inform the public about the conduct of public officials and our government.

B. Defendant Holder used his personal control over his department to create a policy and practice to use the controversial Espionage Act of 1917 to initiate prosecutions of persons

that implicated journalists, including Plaintiffs, who were placed under secret and illegal surveillance. Defendant Holder likewise led an appalling crackdown on whistle-blowers that included personally justifying massive warrantless surveillance over U.S. citizens, including Plaintiffs. Defendant Holder's conduct was not mere supervisory in that he was personally and actively involved in creating policy for illegal surveillance; approving and targeting journalists, including Plaintiffs; ordered, instructed, and directed illegal surveillance techniques and methods against U.S. citizens; and oversaw enforcement of the policies in a manner that was not tacit, but rather direct.

C. As part of the referenced policy, and under the direction of Defendant Holder personally, a policy was created within the DOJ to secretly seize telephone records for more than twenty telephone lines assigned to members of the press core, including Plaintiffs and the Associated Press and its journalists, and also including personal records of journalists' home and cell phones in direct violation of the constitution. In May, 2013, Defendant Holder's misconduct was directly challenged in a letter from the Associated Press' CEO, Gary Pruitt, who described the referenced misconduct as "a massive and unprecedented intrusion by the DOJ into the news-gathering activities" of the press. The misconduct included participation by the very same organization, Verizon, which participated in the subject intrusion into Plaintiffs' personal and home life. The intrusions were carried out by Defendant Holder without notice, without legal authority, and in direct violation of the law. As described by the AP, "(T)here can be no possible justification for such an overbroad collection of the telephone communications of The Associated Press and its reporters. These records potentially reveal communications with confidential sources… provide a road map to AP's newsgathering operations, and disclose information about AP's activities and operations that the government has no conceivable right to know", and also not tied to any particular ongoing investigation or authority.

D. Under the direction of Defendant Holder, and pursuant to his own personal instruction, Deputy Attorney General James Cole, who oversaw the illegal program at the direction of Defendant Holder, responded to the AP letter on May 14, stating that the DOJ carried out the policy and program created by Defendant Holder on grounds that a basis existed to believe certain phone numbers were associated with media personnel involved in reporting classified information.

E. Consistent with the referenced complaints about Holder's personal misconduct, *The Reporters Committee for Freedom of the Press,* along with fifty other news organizations, challenged Defendant Holder's policy and conduct, claiming that Defendant Holder's personal conduct violated the law and far exceeded any alleged police powers, including a failure to balance any government interest with First Amendment rights of the news media and the public's interest in reporting on all manner of government conduct, including Plaintiffs' constitutional liberties and rights.

F. The clear motive behind Defendant Holder's personal misconduct was a desire and intent to illegally silence whistleblowers, adversely impact First Amendment rights of U.S.

citizens, and bring direct harm to Plaintiffs and those similarly situated for political and personal reasons.

G. Defendant Holder, through his own conduct, likewise promulgated a policy that required or encouraged the violation of Plaintiffs' rights, and personally gave instruction to employees and agents to violate the constitution, including Plaintiffs' rights, through the use of illegal surveillance and computer intrusion.

H. Defendant Holder was the principal architect of the illegal policy through his own conduct, which included instructions to agents and employees working with and for him.

I. Defendant Donahoe was instrumental in adopting and executing the plan through his own conduct in providing access to the Postal Service IP address to be used for the inappropriate surveillance activity in direct violation of USPS policies, guidelines, and management requirements.

J. Both Defendants Holder and Donahoe, along with others, controlled the policy and practices and were deliberately indifferent to Plaintiffs constitutional rights and protections, and were reckless, indifferent, malicious, and acted with intent to violate the constitution.

K. Both Defendants are personally responsible for their reckless indifference and intentional conduct in the training, hiring, and supervision over the very agents and representatives they instructed to be involved in the surveillance process. In short, Defendants Holder and Donahoe engaged in conduct that directly caused and subjected Plaintiffs to violations of their constitutional rights.

L. The policy and personal conduct of Defendants Holder and Donahoe were purposefully adopted and carried out with intent of violating Plaintiffs First Amendment rights and, with respect to the Fourth Amendment, the conduct of Defendants was carried out recklessly and with objective unreasonableness.

M. Defendant Holder had actual knowledge, as early as 2009, of the government's use of illegal surveillance techniques, including techniques that were used in criminal investigations in violation of the law. The Inspector General of the Justice Department issued a report on NSA surveillance programs that included recommendations to the DOJ for correction, which shows clear evidence of prior knowledge.

N. In April, 2009, the New York Times reported that the National Security Agency (NSA) intercepted private e-mail messages and phone calls of Americans in recent months on a scale that went far beyond the broad legal limits established by Congress. The reporting indicated that the NSA had been engaged in "overcollection" of domestic communications of Americans, and described the practice as significant and systemic. In response to the inquiries and complaints, Defendant Holder, on behalf of the DOJ,

acknowledged that there had been problems with the NSA surveillance operation, but assured the media that the problems had been resolved, and that Defendant Holder personally went to the national security court to seek a renewal of the surveillance program. Both the House and Senate intelligence committees said at the time that they too had concerns that the DOJ had ignored civil liberties safeguards built into the wiretapping law. As part of the investigation, a senior FBI agent came forward with what the inspector general's office later described as accusations of "significant misconduct" in the surveillance program. The accusations were reported to involve the NSA, in conjunction with DOJ, targeting Americans in eavesdropping operations based on insufficient evidence of involvement in crimes, including an incident where the NSA reportedly took steps to wiretap a member of Congress without a warrant.

O. In further support of Defendant Holder's personal knowledge, in a November 15, 2013, interview, Defendant Holder conceded knowledge of the illegal surveillance techniques being used and publicly represented that the DOJ would re-examine investigations to determine whether warrantless seizure evidence was used improperly by his Agency.

P. The DOJ issued a report based on Defendant Holder's investigation that included an admission of excessive intrusion in that it confirmed that significant revisions to Department policies were being made, further indicative of a federal agency that Defendant Holder had actual knowledge was conducting illegal surveillance in violation of the constitutional rights of journalists.

Q. With regard to the illegal intrusion of Plaintiffs electronics, Defendant Holder was personally involved in monitoring and reviewing the investigative reports produced by Plaintiff Attkisson. For instance, in June, 2011, Eric H. Schultz (the White House) was working closely with Tracy Schmaler, a top aide to Defendant Holder in the DOJ's public affairs office since 2009, directly discussing Plaintiff's reporting on the *Fast and Furious* scandal. During all relevant time periods, Schmaler served as Defendant Holder's personal spokesperson throughout the congressional investigation into ATF's Operation *Fast and Furious*. Defendant Holder has been publicly quoted as recognizing Schmaler as "one of his closest and most trusted advisors …"

R. Defendant Holder shared his disdain for Plaintiff Attkisson's reporting with the White House as well. Documents produced as a result of a lawsuit against DOJ by government watchdog group *Judicial Watch*, to challenge the President's assertion of executive privilege showed Defendant Holder and Schmaler communicating directly with the White House about the investigative reporting by Plaintiff Attkisson, privately referring to it as "out of control".

S. At Defendant Holder's direction, Schmaler later sent an email to White House Deputy Press Secretary Eric Schultz (October 4, 2011) proving that Defendant Holder and Schmaler became so concerned about *muzzling* Plaintiff Attkisson that Schmaler was directed to call Attkisson's editor and longtime CBS anchor Bob Scheiffer to get a

"handle" on her reporting, an overt act taken to control and squash freedom of the press, her professional activities, and for political and personal reasons.

T. In the growing concern within the DOJ, the White House (Eric Schultz) was found to have even communicated that he approved of the call to CBS, stating: "Good. Her [Attkisson] piece was really bad for the AG", further reflecting the panic within the DOJ and the intent to put a stop to Plaintiff's reporting by any means necessary, again for personal and political reasons.

U. The specific story by Plaintiff Attkisson that Defendant Holder, Schmaler and Schultz (the White House) referred to above concerned internal memos showing Defendant Holder was briefed about Operation *Fast and Furious* nearly one year earlier than he admitted to Congress in sworn testimony given in May, 2011.

V. Even more significantly, when the referenced email exchange occurred, the White House publicly denied any discussion about Operation *Fast and Furious* with Defendant Holder or the DOJ. The email not only proves that the DOJ and White House were jointly targeting Attkisson for political and personal reasons, but were working together to mitigate the scandal, halt Plaintiff's reporting, and to seek to use all means necessary to silence her.

W. In addition to going directly to the supervisors of reporters for intimidation purposes, Defendant Holder and partner Schmaler began using the DOJ assets to regularly work with smear machines like *Media Matters* to attack reporters and DOJ whistleblowers. Literally dozens of pages of emails between Schmaler and *Media Matters* staffers show Defendant Holder and Schmaler, Holder's top press defender and partner, worked directly with *Media Matters* to attack reporters, including Plaintiff Attkisson, covering DOJ.

X. As Plaintiffs continued to report on the scandal, tensions rose at the DOJ and White House to the point that Schmaler and White House associate communications director Eric Schultz lost composure and yelled and screamed at Plaintiff Attkisson over her reporting. During this same time frame is when evidence reveals that aspects of the illegal surveillance was initiated against Plaintiffs.

Y. As part of the policy promulgated by Defendant Holder to attack leakers and conduct illegal surveillance of the media, people with knowledge of the inner-workings of the Government have come forward with evidence including that the White House, and NSA, among others, were operating with so-called "Super User"-authorized officials aimed at obtaining authority outside of FISA court and law to carry out operations, both international and domestic, that were illegal, including surveillance that required remotely placing software on a target's computer system, all of which required a so-called "presidential finding" directly from within the White House. These so-called "presidential findings" came complete with cover stories (commonly referred to as a lie

in case the perpetrator was caught), along with terms under which one could continue to do conduct similar operations without constant pre-approval, such as surveillance of target journalists. Additionally, White House "taskers" were assigned to crack down on leakers. The so-called "presidential finding" could be issued by a variety of point-persons located both within the White House, the Vice President's office, as well as a military representative working within the White House National Security Staff.

Z. In further support of Defendant Holder's own personal misconduct, in July, 2013, Defendant Holder delivered a six page report to President Obama informing the President that "he" (Defendant Holder) would create and send new guidelines on dealing with news media to prosecutors, including a dictate that records of a journalist will only be collected if that person is the focus of a criminal investigation and DOJ will forego the opportunity to use search warrants to obtain journalists' emails or other work product, as long as the reporters are engaged in routine newsgathering activities. Needless to say, Defendant Holder would not have needed a new policy had he not previously created and/or maintained a policy that had to be changed, including one that directly violated constitutional freedoms protected by law.

AA. In further support of the claims against Defendant Holder for his own personal misconduct in violating Plaintiffs constitutional rights, on or about May 17, 2013, the Washington Post reported that the DOJ, under the direction of Defendant Holder, previously illegally tracked Fox News reporter James Rosen's visits to the State Department through phone traces, the timing of calls, and a review of his personal email communications in the course of a leak investigation. Most disturbingly, Defendant Holder himself signed off on the search warrant in spring 2010 that identified Rosen as a "possible co-conspirator" in violation of the Espionage Act and authorized seizure of his private emails. Rosen was described as a "flight-risk" to keep him from being informed of the ongoing surveillance. It was reportedly the first time the government had targeted a member of the press in this manner.

BB. In response to the Rosen attack, an editorial board of the *New York Times* publicly noted that "the Obama administration has moved beyond protecting government secrets to threatening fundamental freedoms of the press to gather news." Greg Leslie, legal director for *Reporters Committee for Freedom of the Press* said, "It's incredible…It's the first time we have seen something like this."

CC. In further support of the mental state of Defendant Holder, and completely contrary to his own actions, and just days prior to the revelation about the Rosen subpoena, on May 15, 2015, Defendant Holder denied, under oath, to the House Judiciary Committee that he had ever targeted the press in this manner, stating: "With regard to the potential prosecution of the press for the disclosure of material, that is not something I've ever been involved in, heard of, or would think would be wise policy".

DD. As was later learned, Defendant Holder and the DOJ had even illegally obtained personal

phone records of Rosen's parents as part of the same course of conduct in illegally eavesdropping on the conduct of the media, including Plaintiffs.

EE. Defendant Holder's own personal involvement in the unprecedented violation of the constitutional rights of members of the media, including Plaintiffs, was further documented by NBC when the news organization reported that Defendant Holder himself was personally involved in "signing-off" on search warrants as far back as 2009-2010, under the false representation that such media members were involved as "possible co-conspirators" in carrying out violations of the Espionage Act, including the seizure of private emails from personal computers, which is precisely what transpired in the subject situation as it relates to Plaintiffs.

FF. Defendant Holder's own personal conduct was likewise criticized by Judge Andrew Napolitano who stated that "(T)his is the first time that the federal government has moved to this level of taking ordinary, reasonable, traditional, lawful reporter skills and claiming they constitute criminal behavior", all of which threatened fundamental freedoms of the press to gather news. The conduct of Defendant Holder was felt to be so instrusive and unprecedented that Dana Milibank of the *Washington Post* described Defendant Holder's conduct as involving the use of "technology to silence critics in a way Richard Nixon could only have dreamed of. To treat a reporter as a criminal for doing his job — seeking out information the government doesn't want made public — deprives Americans of the First Amendment freedom on which all other constitutional rights are based."

GG. As part of his plan, policies, and personal misconduct, and despite clear evidence and statements to the contrary, both public and private, Defendant Holder appeared before the House Judiciary Committee in May, 2015, and denied, under oath, that he had ever targeted the press in the manner described, a statement that is now almost unanimously referred to as a material misrepresentation of conduct that was both proven and known in the nation.

HH. All of the foregoing personal conduct of Defendant Holder spans the precise time period of the illegal conduct complained of herein by Plaintiffs. By way of example, Federal ATF (Alcohol Tobacco & Firearm) agent John Dodson was known to be a key whistleblower in the *Fast and Furious*[8] government debacle. Agent Dodson publicly

[8] In May, 2011, House Oversight Committee chairman, California Republican Rep. Darrell Issa and Iowa Republican Sen. Chuck Grassley sent Defendant Holder a letter requesting details about Operation *Fast and Furious*, which had been a failed federal firearms sting operation, which had allowed some 2,000 weapons to reach Mexican drug gangs. Grassley and Issa urged Holder to cooperate and turn over subpoenaed records that would reveal the scope of the alleged government cover-up under his direction. In October, 2011, 7,600 pages of documents were released that Issa claimed indicated Holder was sent memos in regard to Operation *Fast and Furious* earlier than he at first claimed, contradicting Holder's sworn testimony before the House Judiciary Committee in

revealed that the government was trying to find a reason to prosecute him in retaliation for his whistleblowing activities. In fact, Defendant Holder's U.S. Attorney in Arizona, Dennis Burke, was even caught leaking confidential information about Dodson to the press in an attempt to disparage him, all at the direct instructions of Defendant Holder and in support of his policy of silencing freedom of the press. When Congress initiated an investigation into who leaked the confidential information about whistleblower Dodson, and the U.S. Attorney's illegal action was revealed, Burke was forced to resign.

II. During the same time period, former NSA representatives who previously left in protest of the mass privacy violations alleged to be occurring within the agency, came forward and spoke publicly confirming that the Government, including Defendants herein, was targeting journalists using surveillance techniques unique to the Government, further confirming that the DOJ and the agencies operating under it were targeting journalists as part of the paranoia surrounding alleged leakers using unique and state-sponsored technology.

JJ. Although the Director of National Intelligence, James Clapper, testified before the Senate Intelligence Committee in March, 2013, denying the existence of illegal surveillance and data collection of millions of Americans, whistleblower Edward Snowden's revelations in June, 2013, proved Clapper's testimony was false. Facing accusations of perjury from members of Congress, Mr. Clapper sent a letter to the committee chairwoman, Sen. Dianne Feinstein, in July, 2013, apologizing for his "clearly erroneous" remarks made under oath about the secret surveillance and data collection projects being undertaken

KK. Yet more former Government employees continued to come forward providing further support for the existence of such "black ops" programs targeting citizens like Plaintiffs. For instance, Russell Tice, who spent nearly 20 years working in various government agencies, including the Office of Naval Intelligence, Defense Intelligence Agency, and NSA, publicly stepped forward with alleged firsthand knowledge of the targeting of

---

which he claimed he only recently became aware of the Operation. In April, 2012, Issa announced that his committee was drafting a Contempt of Congress resolution against Holder in response to the committee being "stonewalled by the Justice Department." On June 20, 2012, the Oversight Committee voted 23–17 -- along party lines -- to hold Holder in contempt of Congress for not releasing documents the committee had requested. On June 28, 2012, Holder became the first U.S. Attorney General in history to be held in both criminal and civil contempt. He was held, by a bipartisan vote, in contempt by the House of Representatives in a 255–67 vote, with 17 Democrats voting for the measure, 2 Republicans voting against the measure. President Obama and the Justice Department declined to prosecute the attorney general on the contempt charge citing executive privilege. In September 2012, after a nineteen month review, the United States Department of Justice Office of the Inspector General cleared the Attorney General of any wrongdoing with regard to *Fast and Furious*, stating that there was "no evidence" that Holder knew about the operation before early 2011. In August 2014, a federal judge ordered the Justice Department to provide Congress with some of the previously withheld documents that had led Congress to hold Holder in contempt.

journalists for surveillance. Speaking on television in 2009, Mr. Tice confirmed that while serving as an analyst at the NSA, he personally witnessed an agency program that gathered information on U.S. news organizations and journalists.

LL. In addition to the foregoing, and with regard to technological capabilities of the DOJ, NSA, White House, CIA and other government agencies to conduct remote access surveillance of computer systems, in August, 2013, the German magazine *Der Spiegel* reported that it reviewed NSA documents, which had been provided by Mr. Snowden, that provided clear evidence that the agency hacked into a "specially protected" internal communication system at the Qatar-based broadcaster Al-Jazeera, in almost an identical manner as with Plaintiffs intrusion. According to *Der Spiegel*, the NSA documents listed the operation as "a notable success."

MM. After the public was informed of these illegal actions by the Government, especially those aimed at journalists and whistleblowers, President Obama became so concerned about the public appearance of the program that he publicly ordered a review of DOJ procedures for leak investigations, stating that he was concerned that such inquiries chilled journalists' ability to hold the government accountable. But the President made no apology for the scrutiny of the many officials whose records were searched or who had been questioned by the FBI, including Plaintiffs.

NN. One of the most striking recent revelations about the DOJ's pursuit of the media was the disclosure that the DOJ had, during relevant time frames, obtained e-mails from the Google account of James Rosen of Fox News, in which he corresponded with a State Department analyst suspected of leaking classified information about North Korea. Investigators routinely search the e-mails of suspected leakers, but Congress has specifically forbidden the searching of journalists' work product materials unless the reporter was alleged to have committed a crime and without due process of law.

OO. At all times relevant to the subject complaint, Defendant Donahoe and his Postal Service functioned subject to the Network Management Policy with respect to communications. The policy applied to all Postal Service personnel and contracted vendors and to all information resources, technologies, services, and communications that are part of the network. The policy was created in order to provide a formal documented management expectation and intention. The purpose of the policy was to ensure reliability and functionality of the Postal Service Network. The policy provides the foundation for data communication among employees, customers, partners, and supplier in accordance with security and privacy policies and standards.

PP. Management of the postal service network included all network-based protocols, including all IP addresses. The Postal Service network was required to be installed, managed, tracked, and monitored by Telecommunications Services within the Postal Service, all under the direction and control of Defendant Donahoe. Telecommunications network administrators and engineers maintained ownership of all network components

and were charged with responsibility for overseeing any and all connections to the network. In fact, before any person connected to the Postal Information Technology Network (PITN), all devices were required to be formally registered with and approved by Telecommunications Services, and also required to follow Postal Service standards for devices operating on the PITN.

QQ. The Postal Service was likewise required to follow network security policy as defined by the Corporate Information Security policy of the government. Any use that compromised the integrity of the policy was strictly prohibited, including transmitting across the network. Defendant Donahoe was responsible for personally ensuring that these policies and practices were followed and that the operation conducted business in a legal manner.

RR. With respect to "partner" connectivity, any outside connectivity requests were required to be requested through a "sponsor", such as a portfolio manager, program manager, or project manager, and were required to be funded by the requestor's organization. Any such requests were required to be approved by the Postal Service Network Connectivity Board (NCRB) and, ultimately, Defendant Donahoe.

SS. During all times relevant to the subject Complaint, the United States Postal Inspection Service ("USPIS") served as the law enforcement arm of Defendant Donahoe's United States Postal Service. Its jurisdiction was defined by federal law and regulations as "crimes that may adversely affect or fraudulently use the U.S. Mail, the postal system or postal employees." The mission of the U.S. Postal Inspection Service is to support and protect the U.S. Postal Service, its employees, infrastructure, and customers by enforcing the laws that defend the nation's mail system from illegal or dangerous use.

TT. The USPIS was manned with approximately 4,000 employees, 1,200 criminal investigators, an armed uniformed division with 1,000 personnel, forensic laboratories and a communications system, and with 1,000 technical and administrative support personnel, the USPIS leads and assists in numerous joint federal and state investigations.

UU. The Postal Inspection Service operated with the oldest origins of any federal law enforcement agency in the United States. It traced its roots back to 1772, when colonial Postmaster General Benjamin Franklin first appointed a "surveyor" to regulate and audit the mails. Thus, the Service's origins—in part—predate the Declaration of Independence, and therefore the United States itself. As fact-finding and investigative agents, Postal Inspectors are sworn federal law enforcement officers who carry firearms, make arrests and serve federal search warrants and subpoenas. Inspectors work closely with U.S. Attorneys, other law enforcement agencies, and local prosecutors to investigate postal cases and prepare them for court.

VV. The USPIS exists pursuant to Congress's power "to make all Laws which shall be necessary and proper" to perform the obligation provided by the U.S. Constitution "to establish Post Offices and post Roads" (Art. I, § 8, cl. 7). The role of the USPIS is to

safeguard the nation's mail, to protect the integrity of the postal system, and to ensure that the postal system is not used for illegal purposes (President's Commission on the United States Postal Service, 2003, p. 99). It is part and parcel of the USPS and vital to its operation and existence.

WW. Prior to 9/11, USPIS agents participated to varying degrees with the DOJ, and particularly with the Federal Bureau of Investigation's (FBI's) regional Joint Terrorism Task Forces (JTTFs), providing information and assisting with investigations; however, the participation grew substantially following the attack of 9/11. Since 9/11, the USPIS operated with a full-time liaison at the FBI's National JTTF. Also, the USPIS operated with a full-time liaison at DHS's National Operations Center (IS, 2008a), all working directly with the DOJ. The USPIS also routinely collaborated with federal, state, and local law enforcement agencies on a number of interagency task forces. As a consequence, the DOJ and the USPIS/USPS are designed to, and do in reality, operate together as joint venturers, partners, and agents for purposes of certain types of investigations and surveillance.

XX. By way of example of the roles and relationships between the USPS, DOJ, and law enforcement and surveillance powers, an article published in October, 2014, in the *New York Times* reported on the USPS's unconstitutional monitoring of mail. The *Times* noted that "(I)n a rare public accounting of its mass surveillance program, the United States Postal Service reported that it approved nearly 50,000 requests last year from law enforcement agencies, including arms of the DOJ, and its own internal inspection unit to secretly monitor the mail of Americans for use in criminal and national security investigations." The number of requests, contained in a 2014 audit of the surveillance program by the Postal Service's inspector general, showed that the surveillance program was more extensive than previously disclosed and that oversight protecting Americans from potential abuses was lax, all under the direct control, supervision, and policies initiated and controlled by Defendant Donahoe.

YY. At all times relevant to the subject Complaint, Defendant Donahoe was personally responsible for the illegal use of IP addresses assigned to his control, including the IP address found on Plaintiffs' computer system in the subject surveillance matter. Defendant Donahoe had a legal obligation to personally ensure that the IP addresses were not used inappropriately, illegally, or outside the confines of the constitution. In allowing unauthorized access to USPS IP addresses for corrupt purposes, Defendant Donahoe's personal conduct is at direct issue in subjecting Plaintiffs to, or causing them to be subjected to, constitutional violations. As such, Defendant Donahoe is responsible under the law for his own conduct in approving such conduct or, alternatively, in failing to appropriately monitor the IP address system to ensure it was not illegally used.

COUNT 1

VIOLATION OF THE FIRST AMENDMENT TO THE CONSTITUTION

73. Plaintiffs incorporate and re-allege each and every allegation above as if fully set forth herein, including the allegation of the original complaint.

74. This action arises under *Bivens.*[9]

75. Defendants acted under color of law when conducting surveillance on the Plaintiffs and inhibiting the exercise of her First Amendment rights.

76. The surveillance of Plaintiffs' computers and telephones violated the First Amendment to the United States Constitution. By subjecting Plaintiffs to surveillance of her investigative efforts, Defendants sought to abridge the freedom of the pressand chill the exercise of her free speech in a reckless manner with objective unreasonableness, and with the intent to violate their rights.

77. The violation of Plaintiffs' First Amendment rights proximately caused injuries, as set forth herein.

78. By virtue of the foregoing, the Defendants are liable to Plaintiffs for the violation of rights under the First Amendment.

COUNT 2

VIOLATION OF THE FOURTH AMENDMENT TO THE CONSTITUTION

79. Plaintiffs incorporate and re-allege each and every allegation above as if fully set forth herein, including all allegations in the original complaint.

---

[9] See footnote 1.

80. As before, this action arises under *Bivens.*[10]

81. At all times relevant to the subject Complaint, Defendants acted under color of law when conducting surveillance on the plaintiffs.

82. The surveillance of Plaintiffs' computers and telephone violated the Fourth Amendment to the United States Constitution. The Plaintiffs' right to be secure in their person, residence, papers, and effects against unreasonable searches and seizures was violated. The Plaintiffs had a reasonable expectation of privacy with respect to their computers and telephones, and the Defendants had no warrant authorizing the surveillance, nor did any exigent circumstances exist at the time of such surveillance.

83. The violation of the Plaintiffs' Fourth Amendment rights proximately caused their injuries, as set forth herein.

84. The Defendants' acted with reckless and callous indifference to the federally protected rights of the Plaintiffs. Defendants' conduct, among other things, included all actions set forth in paragraph 71 above. That paragraph, including all sub-paragraphs, are hereby incorporated by reference as if repeated in this Count.

85. By virtue of the foregoing, the Defendants are liable to Plaintiffs for their violation of the Plaintiffs' rights under the Fourth Amendment.

---

[10] See footnote 1.

COUNT 3

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVCAY ACT 18 U.S.C. §§ 2511 & 2520

86. All prior allegations are restated herein by reference.

87. The Defendants, individually and in concert, intercepted, endeavored to intercept, and/or procured another person to intercept or endeavor to intercept the Plaintiffs' wire, oral, or electronic communications.

88. The Defendants, individually and in concert, used, endeavored to use, and/or procured another person to use or endeavor to use and electronic, mechanical, or other device to intercept Plaintiffs' oral communications. Such device or devices were affixed to or transmitted a signal through a wire used in wire communications, and was for the purpose of obtaining information relating to business which affects interstate commerce. A substantial part of such conduct occurred in the District of Columbia.

89. The Defendants, individually and in concert, disclosed or endeavored to disclose the contents of Plaintiffs' wire, oral or electronic communications, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communications.

90. Upon information and belief, the above alleged conduct occurred without authorization from a court of competent jurisdiction.

91. As a direct and proximate result of the aforesaid conduct, Plaintiffs have suffered damages as set forth herein.

COUNT 4

VIOLATION OF THE STORED COMMUNICATIONS ACT
18 U.S.C. §§ 2701 & 2707

92. All prior allegations are restated herein by reference.

93. The Defendants, individually and in concert, intentionally accessed and/or caused to be accessed without authorization a facility through which an electronic communication service is provided, and thereby obtained Plaintiffs' wire or electronic communications while they were in electronic storage.

94. As a direct and proximate result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

COUNT 5

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT
18 U.S.C. § 1030

95. All prior allegations are restated herein by reference.

96. The Defendants, individually and in concert, intentionally accessed the Plaintiffs' computers and thereby obtained information from a protected computer, to wit Ms. Attkisson's computers used for her work as an investigative journalist for a national news agency.

97. The Defendants, individually and in concert, knowingly and intentionally accessed and/or caused to be accessed Plaintiffs' protected computers, causing interruption and interference with the ability to use such computers.

98. As a direct and proximate result of the aforesaid conduct, Plaintiffs have suffered damages as set forth herein.

COUNT 6

VIOLATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT
50 U.S.C. § 1810

99. All prior allegations are restated herein by reference.

100. The Plaintiffs were the target of electronic surveillance and/or their communications were subject to electronic surveillance at the hands or direction of the Defendants, and therefore qualify as "aggrieved persons" per 50 U.S.C. 1801.

101. The Plaintiffs were not provided with notice of such surveillance, and upon information and belief such surveillance was not conducted pursuant to authorization from a court of competent jurisdiction.

102. As a direct and proximate result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

COUNT 7

VIOLATION OF THE VIRGINIA COMPUTER CRIMES ACT
VA. CODE § 18.2-152.12

103. All prior allegations are restated herein by reference.

104. The Defendants, individually and in concert, caused the Plaintiffs' computers to malfunction, and used or caused to be used a computer or computer network to make or cause to be made an unauthorized copy of data and communications stored in the Plaintiffs' computers.

105. As a direct and proximate result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

COUNT 8

COMMON LAW TRESPASS TO LAND AND CHATTEL

106. All prior allegations are restated herein by reference.

107. The Defendants, individually and in concert, entered upon or caused others to enter upon the Plaintiffs' property for purposes of installing unauthorized wire surveillance devices to conduct unlawful surveillance upon the Plaintiffs' electronic communications.

108. The Defendants, individually and in concert, intruded upon or caused others to intrude upon the Plaintiffs' personal property, namely computers and other electronic devices, for purposes of conducting unlawful surveillance upon the Plaintiffs' electronic communications.

109. These trespasses to land and chattel were conducted without the Plaintiffs' consent and without lawful authority.

110. As a result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

DAMAGES

111. The Defendants' conduct directly and proximately caused injury to the Plaintiffs in the form of trespass upon and damage to personal property, both real and tangible, workplace harassment and intimidation, fear, stress, embarrassment, expense, inconvenience, and anxiety.

112. In an effort to discover what was happening with Ms. Attkisson's laptop and phone lines, the Plaintiffs were forced to spend a substantial amount of time and expense in investigating the maladies and hiring others to perform forensic investigations.

113. As a journalist, the ability to protect sources is crucial, and Ms. Attkisson's ability to offer such protection was compromised as a result of the surveillance giving rise to this claim.

114. This created a substantial amount of anxiety, jeopardized Plaintiff' success as a journalist, and made Plaintiff Attkisson's job more difficult than it would otherwise have been.

115. Plaintiffs have incurred and will continue to incur attorneys' fees for the prosecution of this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request judgment in their favor against Defendants, Eric H. Holder, individually, Patrick R. Donahoe, individually, Unknown Named Agents of the Department of Justice, Unknown Named Agents of the United States Postal Service, and Unknown Named Agents of the United States, jointly and severally, for compensatory damages in an amount to be proven at trial; for punitive damages in an amount to be proven at trial; for statutory damages pursuant to 18 U.S.C. §§ 1030, 1810, 2520 & 2707, and Virginia Code § 18.2-152.12; for an injunction prohibiting the Defendants, and all other agents of the DOJ and USPS, from conducting surveillance of any sort against Ms. Attkisson without first obtaining a warrant in compliance with the law; for a Declaration that Defendants' actions, practices, customs, and policies regarding the unauthorized surveillance of the Plaintiffs were unjustified, illegal, and violated the constitutional and legal rights; for attorney's fees and costs; and for such other and further relief as the Court may deem just and appropriate.

TRIAL BY JURY IS DEMANDED.

Respectfully Submitted,
SHARYL THOMPSON ATTKISSON
JAMES HOWARD ATTKISSON
SARAH JUDITH STARR ATTKISSON
By counsel

/s/ David W. Thomas
J. Gregory Webb, Esq. (VA Bar No. 38157)
David W. Thomas, Esq. (VA Bar No. 73700)
E. Kyle McNew, Esq. (VA Bar No. 73210)
MichieHamlett PLLC
500 Court Square, Suite 300
Post Office Box 298
Charlottesville, VA 22902-0298
Phone: (434) 951-7200
Fax: (434) 951-7218
dthomas@michiehamlett.com
gwebb@michiehamlett.com
kmcnew@michiehamlett.com

C. Tab Turner, Esq. (Admitted *Pro Hac Vice*)
TURNER & ASSOCIATES, P.A.
4705 Somers Avenue, Suite 100
North Little Rock, Arkansas 72116
501-791-2277 – Office
501-791-1251 – Facsimile
Tab@TTurner.com

CERTIFICATE OF SERVICE

I hereby certify that on September 15, 2017, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing (NEF) to the following counsel of record:

Andrew Han, Esq.
Dennis Carl Barghaan, Jr., Esq.
Lauren A. Wetzler, Esq.
Office of the United States Attorney
Justin W. Williams U.S. Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314
Tel: 703-299-3970
Fax: 703-299-3983
Andrew.han@usdoj.gov
Dennis.barghaan@usdoj.gov
Lauren.wetzler@usdoj.gov
Counsel for Defendants Eric Himpton Holder, Jr., Patrick R. Donahoe, Postal Service, and United States of America

/s/ David W. Thomas
J. Gregory Webb, Esq. (VA Bar No. 38157)
David W. Thomas, Esq. (VA Bar No. 73700)
E. Kyle McNew, Esq. (VA Bar No. 73210)
MichieHamlett PLLC
500 Court Square, Suite 300
Post Office Box 298
Charlottesville, VA 22902-0298
(434) 951-7200; (434) 951-7218 (Facsimile)
dthomas@michiehamlett.com
gwebb@michiehamlett.com
kmcnew@michiehamlett.com